



TITLE:

# On Constant Subrings (Skew Polynomial Rings, Group Rings and Related Topics)

AUTHOR(S):

KISHIMOTO, KAZUO

---

CITATION:

KISHIMOTO, KAZUO. On Constant Subrings (Skew Polynomial Rings, Group Rings and Related Topics). 数理解析研究所講究録 1981, 438: 31-37

ISSUE DATE:

1981-09

URL:

<http://hdl.handle.net/2433/102783>

RIGHT:

# ON CONSTANT SUBRINGS

Kazuo KISHIMOTO

Department of Mathematics, Shinshu University

Throughout,  $A$  will represent a ring with identity element  $1$ , and  $B$  an extension ring of  $A$  with the common identity  $1$ .

A sequence  $L = \{f_0 = 1, f_1, \dots, f_s ; f_i \neq 0\}$  of  $\text{End}(B_A) = \text{Hom}(B_A, B_A)$  is called a derived sequence with an associated sequence (abbr. a.s.) if, for each  $i = 0, 1, \dots, s$ , there exists a sequence  $\{g_{i,0}, g_{i,1}, \dots, g_{i,i}\}$  of  $\text{End}(B_A)$  such that

(i)  $g_{i,0}$  is an isomorphism

(ii)  $f_i(xy) = \sum_{k=0}^i g_{i,k}(x)f_{i-k}(y)$  for  $x, y \in B$ .

(1) If  $\sigma$  is an  $A$ -ring automorphism of  $B$  and  $D$  is a  $\sigma$ -derivation of  $B$  with  $D(A) = 0$ , then  $\{D_0 = 1, D_1 = D, \dots, D_s = D^s \neq 0\}$  is a derived sequence with an a.s.  $\{g(k, i-k) ; k = 0, 1, \dots, i\}$  where  $g(k, i-k)$  is the sum of all different products of  $k$ 's  $D$  and  $i - k$ 's  $\sigma$ . We denote it by  $\mathcal{D}$ .

(2) An iterative higher  $A$ -derivation  $\{d_0 = 1, d_1, \dots, d_s ; d_i \neq 0\}$  (See [2], p. 191) is a derived sequence with an a.s.  $\{g_{i,k} = d_k ; k = 0, 1, \dots, i\}$ . We denote it by  $H$ .

Let  $[L]$  be the multiplicative subsemigroup of  $\text{End}(B_A)$  generated by  $L$ . Then, for any  $\Lambda \in [L]$  and  $b \in B$ ,  $\Lambda b \in \text{End}(B_A)$  by  $\Lambda b(x) = \Lambda(bx)$  ( $x \in B$ ). Moreover, if  $\Lambda = f_i$ ,  $f_i(bx) = \sum_{k=0}^i g_{i,k}(b) f_{i-k}(x)$  shows that

$$f_i \cdot b = \sum_{k=0}^i g_{i,k}(b) f_{i-k}$$

Thus we can see that

$$(*) \quad \Lambda b = \sum_{\Omega} b_{\Omega} \Omega \quad (b_{\Omega} \in B, \Omega \in [L]) \quad \text{for any } \Lambda \in [L].$$

Moreover,  $b_{\Omega}$  is an image of  $b$  under a homomorphism  $g_{\Lambda, \Omega}$  which is a sum of products of  $g_{i,j}$ . Hence we denote  $b_{\Omega} = g_{\Lambda, \Omega}(b)$ .

The purpose of this note is to study relationships between  $B$  and  $A$  when  $L = \mathcal{O}$  or  $H$  and  $A = B^{[L]} = \{b \in B; \Lambda(b) = 0, \Lambda \in [L]\}$ . For this purpose, we put some assumptions on  $L$ .

First, we assume that

$$(a) \quad \Lambda bc = (\Lambda b)c \quad \text{for any } \Lambda \in [L] \text{ and } b, c \in B.$$

Remark I. If  $L = \mathcal{O}, H$ , then  $[L]$  satisfies (a).

Now, we put further assumptions as follows:

(b) There exists a subset  $V = \{(f_1)^{r_1}(f_2)^{r_2} \dots (f_s)^{r_s}; 0 \leq r_i \leq q_i\}$  such that  $(f_1)^{r_1}(f_2)^{r_2} \dots (f_s)^{r_s} \neq 0$  and each  $\Lambda$  of  $[L]$  is obtained by  $n(\Lambda)\Omega$  for some  $\Omega \in V$  and an integer  $n(\Lambda)$ .

(c)  $t = (f_1)^{q_1}(f_2)^{q_2} \dots (f_s)^{q_s}$  is a unique element

in  $V$  such that  $f_i t = 0$  for all  $i = 1, 2, \dots, s$ .

(d) For any  $\Lambda, \Omega \in V$  with  $\Lambda \neq \Omega$ ,  $f_i \Lambda = f_i \Omega$  implies  $f_i \Lambda (= f_i \Omega) = 0$ .

We now consider a free left  $B$ -module  $\Delta = \Delta(B, [L]) = \sum_{\Omega \in V} \oplus Bu(\Omega)$  with a  $B$ -basis  $u(V) = \{u(\Omega) ; \Omega \in V\}$ .

Then  $\Delta$  becomes a ring by the multiplication

(1)  $u(\Lambda)u(\Omega) = n(\Lambda, \Omega)u(\Gamma)$  where  $n(\Lambda, \Omega)$  is an integer such that  $\Lambda\Omega = n(\Lambda, \Omega)\Gamma$ ,  $\Gamma \in V$ .

(2)  $u(\Lambda)b = \sum_{\Omega} g_{\Lambda, \Omega}(b)u(\Omega)$  which is given by (\*).

Remark II. (1) If  $L = \mathcal{D} = \{D_0 = 1, D_1 = D, \dots, D_s (= D^s) \neq 0\}$  and  $D^{s+1} = 0$ , then  $\mathcal{D}$  satisfies (b), (c) and (d).

(2) Let  $L = H = \{d_0 = 1, d_1, \dots, d_s \neq 0\}$  with  $s = p^e - 1$  for some prime  $p$  and  $d_{s+1} = 0$ . Since  $d_i d_j = \begin{cases} \binom{i+j}{i} d_{i+j} & \text{if } i+j \leq s \\ 0 & \text{if } i+j > s, \end{cases}$  if  $A$  is an algebra over  $GF(p)$  then each element of  $[L]$  is obtained by  $n(r_0, \dots, r_{e-1}) \cdot (d_1)^{r_0} (d_p)^{r_1} \dots (d_{p^{e-1}})^{r_{e-1}}$  ( $0 \leq r_i < p$ ) for some integer  $n(r_0, \dots, r_{e-1})$ . Hence  $V = \{(d_1)^{r_0} (d_p)^{r_1} \dots (d_{p^{e-1}})^{r_{e-1}} ; 0 \leq r_i < p\}$  satisfies (b), (c) and (d).

Under these preparations, we shall state several results. The detail of them will be seen latter in papers to appear.

Theorem 1.  $\Delta = \sum_{\Lambda \in V} \oplus u(\Lambda)B.$

It is clear that the map  $j: \Delta \longrightarrow \text{End}(B_A)$  defined by  $j(bu(\Lambda)) : x \longrightarrow b\Lambda(x)$  is a ring homomorphism. Moreover, if we note that  $\text{End}(B_A)$  is a  $\Delta$ -B-module,  $j$  is a  $\Delta$ -B-homomorphism. In the rest, we assume that  $A = B^{[L]}$ . Then, by make use of Theorem 1 and the similar method of [1], we have the following

Theorem 2. Let  $j$  be an isomorphism.

$$(1) \quad j(u(t)B) = \text{Hom}(B_A, A_A)$$

(2) If  $B_A$  is finitely generated projective, then there exist elements  $x_1, x_2, \dots, x_m$  and  $y_1, y_2, \dots, y_m$  in  $B$  such that  $\sum_{i=1}^m x_i g_{t,1}(y_i) = 1$  and  $\sum_{i=1}^m x_i g_{t,\Lambda}(y_i) = 0$  for all  $\Lambda (\neq 1) \in V.$

(3)  $B_A \oplus > A_A$  if and only if there exists an element  $x \in B$  such that  $t(x) = 1.$

A system of elements  $\{x_1, x_2, \dots, x_m ; y_1, y_2, \dots, y_m\}$  of  $B$  which satisfies the condition of (2) is called a  $[L]$ -system for  $B/A$ . Moreover  $B/A$  is called a  $[L]$ -Galois extension if  $B^{[L]} = A$  and  $B$  has a  $[L]$ -system.

Here after, we assume that  $A$  is an algebra over  $\text{GF}(p)$  for a prime  $p$ ,  $\mathcal{D} = \{D_0 = 1, D_1 = D, \dots, D_{p-1} = D^{p-1} \neq 0\}$  with  $D^p = 0$  and  $\sigma D = D\sigma$ ,  $H = \{d_0 = 1, d_1, \dots, d_{p^e-1}\}$  with  $d_{p^e} = 0$ . Then we have the following

Theorem 3. Let  $L = \mathcal{D}$  or  $H$ .

(1)  $B_A$  is finitely generated projective and  $j$  is an isomorphism if and only if there exists a  $[L]$ -system for  $B/A$ .

(2) If  $B/A$  is a  $[L]$ -Galois extension and  $\{x_1, x_2, \dots, x_m; y_1, y_2, \dots, y_m\}$  is a  $[L]$ -system, then  $B = A[x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_m]$ .

Let  $E$  be a derivation of  $A$  and let  $A[X;E] = \{\sum_i X^i a_i; a_i \in A\}$  be a skew polynomial ring of derivation type. Then  $(X + a)^k = \sum_{i=0}^k X^i \binom{k}{i} \Delta_{i-k}(a)$  where  $\Delta_0(a) = 1$  and  $\Delta_h(a) = E(\Delta_{h-1}(a)) + \Delta_{h-1}(a)a$  (See [3]). Then we have the followings by the aid of Theorem 3.

Theorem 4. If  $B/A$  is a  $[\mathcal{D}]$ -Galois extension with  $B_A \oplus > A_A$  and  $|\sigma| \leq p$ , then there exist a derivation  $E$  of  $A$ , elements  $c \in C$  (the center of  $A$ ) and  $a \in A$  such that

(i)  $E(h(c)) = E(a) = 0$

(ii)  $E^p - h(c)E = I_a$  (the inner derivation effected by  $a$ ), where  $h(c) = (\Delta_{p-1} + E\Delta_{p-2} + \dots + E^{p-2}) (a)$ .

Moreover, if this is the case,  $(X^p - Xh(c) - a)A[X;E]$  is a two sided ideal of  $A[X;E]$  and  $B$  is isomorphic to  $A[X;E]/(X^p - Xh(c) - a)A[X;E]$ .

Conversely, if there exist a derivation  $E$  of  $A$ ,

elements  $c \in C$  and  $a \in A$  which satisfy (i) and (ii),  
then  $B = A[x] = A[X;E]/(X^p - Xh(c) - a)A[X;E]$  ( $x = X +$   
 $(X^p - Xh(c) - a)A[X;E]$ ) has an  $A$ -ring automorphism  $\sigma :$   
 $x \mapsto x + c$ , a  $\sigma$ -derivation  $D : x \mapsto 1$  and  $B/A$  is  
a  $[D]$ -Galois extension for  $D = \{D_0 = 1, D_1 = D, \dots, D_{p-1} =$   
 $D^{p-1}\}$  and  $D^p = 0$ .

Theorem 5. If  $B/A$  is a  $[H]$ -Galois extension with  
 $B_A \oplus > A_A$ , then there exist a derivation  $E$  of  $A$  and  
an element  $a \in A$  such that

- (i)  $E^{p^e} = I_a$
- (ii)  $E(a) = 0$

Moreover, if this is the case,  $(X^{p^e} - a)A[X;E]$  is  
a two sided ideal of  $A[X;E]$  and  $B$  is isomorphic to  
 $A[X;E]/(X^{p^e} - a)A[X;E]$ .

Conversely, if there exist a derivation  $E$  of  $A$  and  
an element  $a \in A$  which satisfy (i) and (ii), then  $B =$   
 $A[x] = A[X;E]/(X^{p^e} - a)A[X;E]$  ( $x = X + (X^{p^e} - a)A[X;E]$  has  
an iterative higher derivation  $H = \{d_0 = 1, d_1, \dots, d_{p^e-1}\}$   
with  $d_{p^e} = 0$  such that  $d_i(x^j) = \begin{cases} \binom{j}{i} x^{j-i} & \text{if } j \geq i \\ 0 & \text{if } j < i \end{cases}$   
and  $B/A$  is a  $[H]$ -Galois extension.

## References

- [1] F.DeMeyer: Some notes on general Galois theory of rings, Osaka J. Math., 2(1965), 117 - 127.
- [2] N. Jacobson: Lectures in abstract algebras III, van Nostrand, 1964.
- [3] K. Kishimoto: On abelian extensions of rings I, Math. J. Okayama Univ., 14(1970), 159 - 174.